DETAILED ACTION

1. This is in response to the amendment filed on 2 March 2010.

2. Claims 1, 5, 7-10, 13, 16-20, 25, 28, 30-33, 36, 37, 40-44, 47, 49-52, 55-61, 64, 66-69, 72-74 and 98-114 are pending in the application.

3. Claims 25, 28, 30-33, 36, 37 and 106-108 have been rejected.

4. Claims 1, 5, 7-10, 13, 16-20, 40-44, 47, 49-52, 55-61, 64, 66-69, 72-74, 98-105 and 109-114 have been allowed.

5. Claims 2-4, 6, 11, 12, 14, 15, 21-24, 26, 27, 29, 34, 35, 38, 39, 45, 46, 48, 53, 54, 62, 63, 65, 70, 71 and 75-97 have been cancelled.

Response to Arguments

6. Applicant's arguments with respect to claims 25, 28, 30-33, 36, 37 and 106-108 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

7. Claim 1 is objected to because of the following informalities: repeated word. The word "the" has been used consecutively in the last limitation. Appropriate correction is required.

Allowable Subject Matter

8. Claims 1, 5, 7-10, 13, 16-20, 40-44, 47, 49-52, 55-61, 64, 66-69, 72-74, 98-105 and 109-114 are allowed.

As to independent claim 1, prior art does not disclose, teach or fairly suggest receiving first data segment; identifying at least two portions of the first data segment including a first portion and a second portion; generating a first hash value from the first portion of the first data segment; identifying a first encryption scheme from among a plurality of encryption schemes the

first encryption scheme being identified by the first hash value corresponding to the first portion of the first data segment; and encrypting, with a computer processor, at least a part of the first data segment using the first encryption scheme.

As to independent claim 40, prior art does not disclose, teach or fairly suggest an input buffer adapted to receive a data segment; a controller coupled to said input buffer, said controller being adapted to generate a first hash value from a first portion of the data segment and to dynamically select a first encryption scheme from a plurality of encryption schemes, each encryption scheme comprising an encryption algorithm and an encryption key, and the first encryption scheme corresponding to the first hash value; an encryption module coupled to the controller and configured to utilize a computer processor to encrypt a second portion of the data segment using the first encryption scheme and an output buffer coupled to said encryption module, said output buffer being adapted to output encrypted data corresponding to the data segment.

As to independent claim 58, prior art does not disclose, teach or fairly suggest an input buffer adapted to receive an encrypted data segment; a controller coupled to said input buffer, said controller being adapted to generate a first hash value from a first portion of the data segment and to dynamically select a first encryption scheme from a plurality of encryption schemes each encryption scheme comprising an encryption algorithm and an encryption key and the first encryption scheme corresponding to the first hash value; a decryption module coupled to the controller and configured to utilize a computer processor to decrypt a second portion of the encrypted data segment using the first encryption scheme; and an output buffer coupled to said

decryption module, said output buffer being adapted to output decrypted data corresponding to the encrypted data segment.

As to independent claim 98, prior art does not disclose, teach or fairly suggest receiving a data segment; selecting an unencrypted first portion, an unencrypted second portion, and an unencrypted third portion of the data segment; generating a first hash value from the unencrypted first portion of the data segment; associating each of a plurality of potential hash values with a corresponding encryption scheme belonging to a plurality of encryption schemes; identifying a first encryption scheme of the plurality of encryption schemes, the first encryption scheme corresponding to a potential hash value that matches the first hash value; encrypting, with a computer processor, the unencrypted second portion of the data segment to provide an encrypted second portion by applying the first encryption scheme; generating a second hash value from the unencrypted second portion of the data segment; identifying a second encryption scheme of the plurality of encryption schemes, the second encryption scheme corresponding to a potential hash value that matches the second hash value; encrypting the unencrypted third portion of the data segment to provide an encrypted third portion by applying the second encryption scheme; and outputting an encrypted data segment corresponding to the data segment, the encrypted data segment comprising the unencrypted first portion, the encrypted second portion, and the encrypted third portion of the data segment.

As to independent claim 101, prior art does not disclose, teach or fairly suggest receiving an encrypted data segment comprising an unencrypted first portion, an encrypted second portion, and an encrypted third portion; generating a first hash value from the unencrypted first portion of the encrypted data segment; associating each of a plurality of potential hash values with a

corresponding encryption scheme belonging to a plurality of encryption schemes; identifying a first encryption scheme of the plurality of encryption schemes, the first encryption scheme corresponding to a potential hash value that matches the first hash value; decrypting, with a computer processor, the encrypted second portion of the encrypted data segment to provide an unencrypted second portion by applying the first encryption scheme; generating a second hash value from the unencrypted second portion of the data segment; identifying a second encryption scheme of the plurality of encryption schemes, the second encryption scheme corresponding to a potential hash value that matches the second hash value; decrypting the encrypted third portion of the data segment to provide an unencrypted third portion by applying the second encryption scheme; and outputting an decrypted data segment corresponding to the encrypted data segment, the decrypted data segment comprising the unencrypted first portion, the unencrypted second portion, and the unencrypted third portion.

Any claims not directly addressed are allowed on the virtue of their dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 25, 28, 30, 32, 33 and 106-108 are rejected under 35 U.S.C. 102(b) as being anticipated by Kawano et al U.S. Patent No. 5,995,623 (hereinafter Kawano).

As to claim 25, Kawano discloses a method for cryptographically processing data, the method comprising:

receiving a first encrypted data segment (i.e. segmented data) [see figure 9a];

identifying at least two portions of the first encrypted data segment, including a first portion and a second portion [see figure 9a];

generating a first hash value from the first portion of the first encrypted data segment (i.e. hash value computed from encrypted portion) [column 15 line 42];

identifying a first encryption scheme from among a plurality of encryption schemes, the first encryption scheme being identified by the first hash value corresponding to the first portion of the first encrypted data segment (i.e. a setoff encryption key and the hash value is computed and is registered in a hash table) [column 15, lines 43-45]; and

decrypting, with a computer processor, at least part of the first encrypted data segment using the first encryption scheme (i.e. the decryption key is taken from hash table) [column 16, lines 12-15].

As to claim 28, Kawano discloses the method of claim 25, further comprising:

providing an encryption table (i.e. hash table) for selecting an encryption scheme from a hash value, the encryption table comprising:

an encryption type identifier [as shown in figure 9b];

an encryption key for the encryption type [as shown in figure 9b]; and

an encryption parameter [as shown in figure 9b],

for each entry associated with a potential hash value corresponding to the first portion of the first encrypted data segment [as shown in figure 9b].

As to claim 30, Kawano discloses the method of claim 25, further comprising:

receiving an encrypted data stream comprising the first encrypted data segment and a plurality of additional encrypted segments, each of the first encrypted data segment and the plurality additional encrypted data segments corresponding to a data packet of the encrypted data stream (i.e. different portions are encrypted with different keys) [column 14, lines 57-67].

As to claim 32, Kawano discloses that the first portion of the first encrypted data segment being an Internet Protocol (IP) header of the first encrypted data segment [column 14, lines 41-53].

As to claim 33, Kawano discloses that the second portion of the first encrypted data segment being one of:

a selected portion of a data field of the data packet (i.e. different portions being encrypted with different keys) [column 14, lines 57-67];

a Transmission Control Protocol (TCP) header of the data packet; and

a User Datagram Protocol (UDP) header of the data packet.

As to claim 106, Kawano discloses the method of claim 25, further comprising:

generating a second hash value from the second portion of the first encrypted data segment [column 16, lines 28-39];

identifying a second encryption scheme from among the plurality of encryption schemes, the second encryption scheme being identified by the second

hash value corresponding to the second portion of the first encrypted data segment [column 16, lines 28-39]; and

decrypting a third portion of the first encrypted data segment using the second encryption scheme [column 16, lines 48-61];

wherein the second portion of the first data segment is decrypted with the first encryption scheme identified by the first hash value corresponding to the first portion of the first encrypted data segment [column 16, lines 48-61].

As to claim 107, Kawano discloses that identifying a first encryption scheme from among the plurality of encryption schemes comprises:

locating the first hash value in an encryption table configured to map a plurality of values to a plurality of encryption schemes (i.e. hash table) [see figure 9b]; and

identifying the first encryption scheme as corresponding to the first hash value in the encryption table [see figure 9b].

As to claim 108, Kawano discloses the method of claim 25, further comprising:

receiving a plurality of additional data segments [column 16, lines 48-61]; and

decrypting the plurality of additional data segments using a plurality of encryption schemes identified by hash values corresponding to portions of the plurality of additional data segments [column 16, lines 48-61].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kawano et al U.S. Patent No. 5,995,623 (hereinafter Kawano) as applied to claim 25 above, and further in view of Robinson et al US 2006/0140197 A1 (hereinafter Robinson).

As to claim 31, Kawano does not teach that the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

Robinson teaches a segment of data for a first protocol layer (i.e. network layer) [0045]. Robinson teaches a segment of data for a second protocol layer (i.e. transport layer) [0046]. The network layer is lower than the transport layer.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kawano so that the first predetermined portion would have contained data for a first protocol layer, and the second predetermined portion would have contained data for a second protocol layer, wherein the first protocol layer was lower than the second protocol layer.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kawano by the teaching of Robinson because it provides a method for recovering data lost in a transmission and is useful for improving the reliabitly of data unit delivery [0002].

11. Claims 36 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawano et al U.S. Patent No. 5,995,623 (hereinafter Kawano) as applied to claim 25 above, and further in view of Tomori et al U.S. Patent No. 6,865,658 B2 (hereinafter Tomori).

As to claims 36 and 37, Kawano does not teach reading the plurality of encrypted data segments from corresponding sectors in a data storage device. Kawano does not teach that the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

Tomori teaches storing and reading data segments from sectors in a data storage device [column 20 line 56 to column 21 line 2; column 24, lines 48-57].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kawano so that the plurality of encrypted data segments would have been read from corresponding sectors in a data storage device. The first predetermined portion would have been a first selected portion in a sector in a data storage device, and the second predetermined portion would have been a second selected portion in the sector.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kawano by the teaching of Tomori because it provides the advantage of providing a data management system and data management method where data divided in units of a sector is stored together with data link information in a plurality of separately distributed sectors of a data storage region, so that the data storage region can be more efficiently utilized [column 16, lines 30-35].

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2431